AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name and authentication level, the method comprising:

(a) on a first graphic user interface of a device, displaying a name conflict indicator next to a first display name that is associated with a first identity, the first identity being different than at least one second identity associated with at least one second display name, the at least one second display name being equivalent to the first display name;

(b) in response to user input associated with the name conflict indicator, displaying on the device a plurality of equivalent display names that are equivalent to the first display name;

(c) receiving user input from a user of the device ~~selecting~~ specifying an alternative display name for a selected display name, the ~~alternative~~ selected display name being selected by the user from the plurality of equivalent display names displayed on the device, the ~~selected~~ alternative display name being associated with a selected identity and being different than the first display name; [[and]]

(d) identifying on a second graphic user interface of the device the selected identity with the alternative display name, the second graphic user interface providing a function related to controlling communication within the peer-to-peer collaboration system, the communication being between the device and a second device associated with the selected identity[[.]];

(e) determining the behavior of the collaboration system regarding communications with a contact based on a security policy and the authentication level of that contact; and

(f) warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

2. (Original) The method of claim 1 wherein step (a) comprises computing a clean name from each display name and comparing clean names of two display names to determine if the two display names are equivalent.

3. (Currently amended) The method of claim 1 ~~wherein each contact identity has an authentication level associated therewith and~~ wherein step (a) comprises:

(a1) examining the authentication levels of all display names that are equivalent; and

(a2) displaying name conflict indicators next to ~~selected~~ display names based on the examination in step (a1).

4. (Original) The method of claim 3 wherein step (a2) comprises displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display names or (2) equals the highest authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

5. (Canceled)

6. (Currently amended) The method of claim [[5]] 1 further comprising:

~~(f)~~ (g) receiving from a user of the collaboration system input specifying the security policy.

7. (Currently amended) The method of claim [[5]] 1 further comprising:

~~(f)~~ (g) receiving from a system administrator input specifying the security policy.

8. (Canceled)

9. (Currently amended) The method of claim [[5]] 1 further comprising:

~~(f)~~ (g) preventing a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

10. (Previously Presented) The method of claim 1 wherein step (b) comprises displaying a dialog box having all display names that are equivalent to the first display name listed therein.

11. (Previously Presented) The method of claim 1 wherein step (c) comprises assigning the alternative display name as an alias to the selected display name which alias is not equivalent to either of the first and second display names and which alias replaces the selected display name.

12. (Currently amended) The method of claim 1 further comprising:

~~(e)~~ (g) displaying an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

13. (Original) The method of claim 12 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

14. (Previously presented) A method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

(a) setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

(b) receiving from a user through a graphic user interface on a display an indication of a selected contact with which to communicate;

(c) obtaining the authentication and certification level of the selected contact; and

(d) presenting on the display information constituting a warning to the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level.

15. (Original) The method of claim 14 wherein step (a) comprises a user setting the security policy that applies to that user.

16. (Original) The method of claim 14 wherein step (a) comprises a system administrator setting a security policy that applies to a user.

17. (Previously Presented) The method of claim 14 wherein step (d) comprises warning a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

18. (Previously Presented) The method of claim 14 wherein step (d) comprises preventing a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

19. (Previously Presented) The method of claim 14 wherein step (d) comprises allowing a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

20. (Previously Presented) The method of claim 14 wherein step (c) comprises:

(c1) compiling a contact list of contacts with whom the user is attempting to communicate;

(c1) checking the contact list to determine contacts that are not authenticated;

(c3) checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

(c4) placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

21. (Currently amended) Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name and authentication level, the apparatus comprising:

means for displaying on a first graphic user interface of a device, a name conflict indicator next to a first display name that is associated with a first identity, the first identity being different than at least one second identity associated with at least one second display name, the at least one second display name being equivalent to the first display name;

means responsive to user input associated with the name conflict indicator for displaying on the device a plurality of display names that are equivalent to the first display name;

means for receiving user input from a user of the device ~~selecting~~ specifying an alternative display name for a selected display name, the ~~alternative~~ selected display name being selected by the user from the plurality of equivalent display names displayed on the device, the ~~selected~~ alternative display name being associated with a selected identity and being different than the first display name; [[and]]

means for identifying on a second graphic user interface of the device the selected identity with the alternative display name, the second graphic user interface providing a function related to controlling communication within the peer-to-peer collaboration system, the communication being between the device and a second device associated with the selected identity[[.]];

a mechanism that provides a security policy that determines the behavior of the collaboration system regarding communications with a contact based on the authentication level of that contact; and

a mechanism that warns a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

22. (Original) The apparatus of claim 21 wherein the means for displaying a name conflict indicator comprises a mechanism that computes a clean name from each display name and a comparator that compares the clean names of two display names to determine if the two display names are equivalent.

23. (Currently amended) The apparatus of claim 21 ~~wherein each contact identity has an authentication level associated therewith and~~ wherein the means for displaying a name conflict indicator comprises:

means for examining the authentication levels of all display names that are equivalent; and

means for displaying name conflict indicators next to selected display names based on display names that are determined to be equivalent by the means for examining the authentication levels.

24. (Original) The apparatus of claim 23 wherein the means for displaying name conflict indicators next to selected display names comprises means for displaying a name conflict indicator next to each display name associated with a contact identity whose authentication level (1) is less than the highest authentication/certification level of all contact identities with equivalent display

names or (2) equals the highest authentication/certification level to which at least two contact identities with equivalent display names have equal authentication levels.

25. (Canceled)

26. (Currently amended) The apparatus of claim [[25]] 21 wherein a mechanism that provides the security policy comprises a mechanism that allows a user of the collaboration system to determine the security policy.

27. (Currently amended) The apparatus of claim [[25]] 21 wherein the mechanism that provides the security policy comprises a mechanism that allows a system administrator to determine the security policy.

28. (Canceled)

29. (Currently amended) The apparatus of claim [[25]] 21 further comprising:
a mechanism that prevents a user from communicating with another user based on the security policy when the other user has a predetermined authentication level.

30. (Original) The apparatus of claim 21 wherein the means for displaying all display names that are equivalent to the selected display name comprises means for displaying a dialog box having all display names that are equivalent to the selected display name listed therein.

31. (Original) The apparatus of claim 21 wherein the a mechanism that resolves the name conflict comprises a mechanism for assigning an alias to one of the first and
second display names which alias is not equivalent to either of the first and second display names and which alias replaces the one display name.

32. (Original) The apparatus of claim 21 further comprising:

a mechanism that displays an authentication indicator next to a display name that is not equivalent to another display name, which authentication indicator displays the authentication level of the associated contact.

33. (Original) The apparatus of claim 32 wherein each contact can have one of a predetermined number of authentication levels and wherein the authentication indicator that is displayed is unique to one of the authentication levels.

34. (Previously presented) Apparatus for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, comprising:

a mechanism that sets a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

means for receiving through a graphic user interface on a display an indication of a selected contact with which to communicate;

means for obtaining the authentication and certification level of the selected contact; and

a mechanism that presents on the display information constituting a warning to the user and restricts the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level based on the security policy.

35. (Original) The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a user to set the security policy that applies to that user.

36. (Original) The apparatus of claim 34 wherein the mechanism that sets the security policy comprises a mechanism that allows a system administrator to set a security policy that applies to a user.

37. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that warns a user when the security policy is set to warn and the user attempts to communicate with an unauthenticated and uncertified contact.

38. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that prevents a user from communicating with an uncertified contact when the security policy is set to restrict and the user attempts to communicate with an uncertified contact.

39. (Original) The apparatus of claim 34 wherein the mechanism that warns the user and restricts the user comprises a mechanism that allows a user to communicate with an unauthenticated and uncertified contact when the security policy is set to allow without warning and the user attempts to communicate with an unauthenticated and uncertified contact.

40. (Previously Presented) The apparatus of claim 34 wherein the means for obtaining the authentication and certification level comprises:

means for compiling a contact list of contacts with whom the user is attempting to communicate;

means for checking the contact list to determine contacts that are not authenticated;

means for checking the unauthenticated contacts to determine whether a certification policy applies to any unauthenticated contact; and

means for placing an unauthenticated contact on the list of unauthenticated and uncertified contacts when no certification policy applies to that contact.

41. (Currently amended) A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple identities each with an associated display name and authentication level, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for displaying on a first graphic user interface of a device a name conflict indicator next to a first display name that is associated with a first identity different than at least one second identity associated with at least one second display name, the at least one second display on the device name being equivalent to the first display name;

program code operable in response to user input from a user of the device associated with the name conflict indicator for displaying a plurality of display names that are equivalent to the first display name;

program code for receiving user input ~~selecting~~ specifying an alternative display name for a selected display name, the ~~alternative~~ selected display name being selected by the user from the plurality of equivalent display names displayed on the device, the ~~selected~~ alternative display name being associated with a selected identity and being different than the first display name; [[and]]

program code for identifying on a second graphic user interface of the device the selected identity with the alternative display name, the second graphic user interface providing a function related to controlling communication within the peer-to-peer collaboration system the communication being between the device and a second device associated with the second identity[[.]];

program code for providing a security policy that determines the behavior of the collaboration system regarding communications with a contact based on the authentication level of that contact; and

program code for warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.

42. (Previously presented) A computer program product for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level, the computer program product comprising a computer usable medium having computer readable program code thereon, including:

program code for setting a security policy that controls the behavior of the collaboration system based on the authentication and certification level;

program code for receiving through a graphic user interface on a display an indication of a selected contact with which to communicate;

program code for obtaining the authentication and certification level of the selected contact; and

program code for presenting on the display information constituting a warning to the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level based on the security policy.